Substitute Abstract

A crypto-processing method capable of confronting an attack, which intentionally causes an erroneous operation and takes out secret information to be done against a device which performs a crypto-processing inside the device such as an IC card. The solution means for such an attack is shown below. A ciphertext C is received through the I/O port on an IC card, etc., the ciphertext C is stored on a RAM, a decryption process of the ciphertext C is performed, and the processing result Z is stored on a RAM. For the processing result Z, an encryption process is executed, and the processing result W and the original plaintext C are compared with each other. When the processing result W coincides with the original plaintext C, the plaintext Z is output to the I/O port, and if not, a reset is effected.